UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/555,301	05/26/2000	MARKUS FEUSER	PHD99-097	3809

7590 11/30/2004

Philips Electronics North American Corp.
580 White Plains Rd.
Tarry town, NY 15091

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/555,301	FEUSER, MARKUS	
	Examiner	Art Unit	
	Beemnet W Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 September 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *5-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The request filed 01 September 2004 for a request for Continued Examination (RCE) under 35 CFR 132 based on parent Application 09/555,301 is acceptable and an RCE has been established. An Action on the RCE follows. Claims 1-4 have been cancelled. New Claims 5-20 have been entered. Drawings filed on 4/5/2004 are acceptable. Claims 5-20 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claim 5-13 and 16-19 is rejected under 35 U.S.C. 102(e) as being anticipated by Reiner (US Patent No. 5,995,629).

4. As per claim 5, Reiner teaches a method of performing calculations and data transfers, comprising:

performing arithmetic operations in a processor substantially continuously, the arithmetic operations including functional operations and dummy operations (i.e., the encoding unit VE continuously generates out put data, where actual arithmetic operations are executed during a

first period of time and after the first time period ends, the integrated circuit continues to generate output data, that are no longer written into the output register, (dummy operations), see column 4, lines 7-29), transferring data between the processor and a first register, the data including select data associated with functional operations and dummy data associated with dummy operations (selectively transferring actual data based on signal ST1 and ST2 within encoding unit VE to register SR and from SR to output register AR, see figure 1 and column 4, lines 7-29) selectively transferring the selected data between the first register and a second register, and transferring the selected data between the second register and other component (transferring data between registers SR (register 1), AR1 (register 2), and AR2), see column 4, lines 53-67, column 5, lines 1-10 and figure 2), wherein dummy operations are performed during gaps in the functional operations so as to mask the power consumptions associated with the functional operations [column 4, lines 7-29 and column 2, lines 12-17].

5. As per claims 6, 10 and 17, Reiner teaches an integrated circuit comprising:

a processor [figure 1, unit VE];

a first data register that is coupled to the processor [figure 1, unit SR];

a second data register that is coupled to the first data register and is configured to transfer data between the first data register and the second data register and between the second data register and other component [figure2, Register AR1, AR2, and ARn];

a controller [figure 1, unit Z, with st1 and st2];

wherein the processor is configured to:

perform a given set of functional operations to execute an intended algorithm during a first time sequence, and transfer data between the processor and the first data register while performing the given set of functional operations (i.e., actual arithmetic operations

executed during a first time period and data transmission performed within a second time period, wherein second time period lies within the first time period) [column 2, lines 24-29 and column 4, lines 7-29],

Furthermore, Reiner teaches transferring data at the second register in a second time sequence that is substantially uncorrelated with the first time sequence, so that a correlation of first currents associated with performing the given set of functional operations and second currents associated with performing the data input and data output transfers related to the given set of functional operations cannot be determined (i.e., actual arithmetic operations executed during a first time period and data transfer from encoding unit to output register performed within a second time period, wherein second time period lies within the first time period, Note that output register is composed of a number of registers AR1 to ARn, (data transfer from register AR1 to AR2 and from AR2 to other component occurs within the second time period), thereby disguising power consumption) [column 2, lines 7-29, column 4, lines 7-29, 53-67].

6. As per claims 7, 16 and 18, Reiner teaches the method as applied above. Furthermore, Reiner teaches the method wherein the functional operations correspond to a cryptography algorithm (encoding operations) [column 3, lines 17-27].

7. As per claim 8, Reiner teaches the method as applied above. Furthermore, Reiner teaches performing the arithmetic operations, transferring the data, and transferring the select data are arranged to substantially mask power consumption related to performing the functional operations [column 4, lines 29-40].

8. As per claim 9, Reiner teaches the method as applied above. Furthermore, Reiner teaches performing arithmetic operations, transferring the data, and transferring the select data are arranged to consume substantially uniform power consumption [column 4, lines 29-40].

9. As per claims 11, 12 and 19, Reiner teaches the controller (Z) configured to control the processor (VE) to execute dummy operations that do not affect the select data during gaps in the first sequence [column 4, lines 13-24].

10. As per claim 13, Reiner teaches the controller is configured to control the processor and to transfer the data so as to substantially mask power consumption variations related to functional operations [column, lines 29-40].

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 14, 15 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reiner (US Patent No. 5,995,629).

13. As per claims 14, 15 and 20, Reiner teaches the integrated circuit as applied above. Furthermore, Reiner teaches performing the arithmetic operations, transferring data between

the processor and registers RA1-RAn, and transferring a select data are arranged to substantially mask power consumption related to performing the functional operations [column 4, lines 29-40]. Reiner, further teaches executing dummy operations that do not affect the select data during gaps in of actual operations [column 4, lines 13-24]. Reiner does not explicitly teach transferring dummy data between the first register and second register. However, It would have been obvious to one having ordinary skill in the art at the time the invention was made to incorporate a method of transferring dummy data between the first register and the second register. It would have been obvious because Reiner teaches execution of actual operations on one hand and data transfer on the other hand executed in parallel [column 4, lines 7-29, column 2, lines 24-29] and generating dummy data on one hand and performing data shifting on the other hand, in parallel [column 4, lines 13-24], which has the advantage of disguising power consumption. Based on this teaching it would have been obvious to one having ordinary skill in the art at the time the invention was made to transfer dummy data between the first register and second register, in order to disguise power consumption.

Response to Arguments

14. With respect to claims 5, 10 and 17, Applicant argues that Reiner does not teach performing operations substantially continuously, and Reiner does not teach the use of additional buffer/register to isolate the times of data transfer from the times of executing. The examiner respectfully disagrees.

Reiner teaches performing arithmetic operations in a processor substantially continuously, the arithmetic operations including functional operations and dummy operations (i.e., the encoding unit VE continuously generates out put data, where actual arithmetic

operations are executed during a first period of time and after the first time period ends, the integrated circuit continues to generate output data, that are no longer written into the output register, (dummy operations), see column 4, lines 7-29). Furthermore, Reiner teaches an out put register (AR) to transfer data from the encoding unit, where the output register AR includes several registers AR1, AR2,..ARn, used as additional buffer [column 4, lines 53-67 and figure 2].

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a) US Patent 5,944,833 to Ugon teaches Integrated circuit and method for decorrelating an instruction sequence of a program.

b) US patent 5,991,415 to Shamir teaches a method and apparatus for protecting public key schemes from timing and fault attacks.

c) US Patent 5,729,766 to Cohen teaches system for memory unit receiving pseudo-random delay signal operative to access memory after delay and additional delay signal extending from termination of memory access

d) US Publication 2002/0084333 to Nakano teaches Data processing apparatus and memory card that out puts pseudo data.

e) US Patent 6,035,368 to Habib teaches a protection method against eeprom-directed intrusion into a mobile communication device that has a processor, and a device having such protection mechanism.

f) US Patent 6,023,776 to Ozaki teaches a central processing unit having a register which store values to vary wait cycles.

g) US Patent 6,581,842 to Sedlak et al teaches Data carrier with regulation of the power consumption.

h) US Patent 4,584,665 to Vrielink teaches an arrangement for protecting against the unauthorized reading of program words stored in a memory.

i) US Patent 6,776,455 to Ryan Jr., teaches System and method for preventing differential power analysis attacks (DPA) on a cryptographic device.

j) US Patent 6,327,661 to Kocher et al teaches Using unpredictable information to minimize leakage from smartcards and other cryptosystems.

k) US Patent 6,615,354 to Ohki et al teaches a method where a relation between a data process contents in an IC card chip and the consumption current of the IC card chip is reduced.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100